

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE HONORABLE BOARD OF PATENT APPEALS

In re application of:)	
)	
Glenn Langford)	
)	Group Art Unit: 2131
Serial No.: 09/746,015)	
)	Examiner: Abrishamkar, Kaveh
Filed: December 26, 2000)	
)	Attorney Docket: 77666-8
For: KEY RELEASE SYSTEMS,)	
COMPONENTS AND METHODS)	

APPEAL BRIEF UNDER 37 C.F.R. 41.37

The Assistant Commissioner of Patents
Washington, D.C. 20231
U.S.A.

Dear Sir or Madam:

In response to the "Order Returning Undocketed Appeal to Examiner" dated July 22, 2008, Applicant submits the following paper providing a summary of the claimed subject matter, which is in compliance with Manual of Patent Examining Practice (MPEP) 1205.03.

It is alleged that the "Summary of Claimed Subject Matter" section appearing on pages 3-5 of the Appeal Brief submitted on May 18, 2007 is deficient. Claims 35 to 42 are alleged to contain "means for" language. It is requested that an explanation of the claims subject matter for claims 35-42 must be mapped to the specification by page and line number.

Applicant notes that claim 33 also includes "means for" language. The Appeal Brief filed May 18, 2007 has a description for claim 33, which has not been objected to.

However, Applicant has elaborated on the description of claim 33 included in the “Summary of Claimed Subject Matter” section of the May 18, 2007 Appeal Brief. Similarly, claim 38, another independent claim which had a description included in the “Summary of Claimed Subject Matter” section of the previously filed Appeal Brief, has been elaborated upon for clarity.

Applicant submits that claim 36 is dependent upon independent claim 33, but does not include any additional “means for” language. Furthermore, claims 39 and 40 are dependent upon independent claim 38, but do not include any additional “means for” language. As claims 36, 39 and 40 are dependent claims that include no “means for” language beyond that of the claims they depend upon, Applicant submits that no detailed description and/or mapping of page and line numbers of claims 36, 39 and 40 is required by 37 CFR 41.37(c)(v).

Summary of Claimed Subject Matter

Claim 33 is directed to a decryptor, an example of which is shown in Figure 1 identified with reference character 12 or shown in Figure 3 also identified with reference character 12. A corresponding description of Figure 3 starts at the bottom of page 12 of the present application. Furthermore on page 10, lines 29-31, a decryptor is described as “any combination of one or more devices and/or software which together are capable of performing decryption operations”. Therefore, Applicant submits that the various “means” recited subsequently may be implemented as devices and/or software.

The decryptor comprises “means for obtaining an encryption block”, an example of which is described at page 12, lines 29-31, in particular with reference to an “input through which it receives an encryption block 56”. The encryption block (reference character 56 in Figure 3), as recited in claim 33, comprises a data ciphertext (reference character 44 in Figure 3) that requires a decryption key to decrypt. The encryption block further comprises key related information (page 18 lines 8 to 13 and page 11, lines 8-33) associated with a first {public key, private key} pair and a key ciphertext consisting of the decryption key encrypted by the first public key. The encryption block does not include an ACD (access controlled decryption) block, as disclosed at page 11, lines 5-7.

The decryptor comprises “means for generating a key release request ... and outputting the key release request to the key release agent”, an example of which is illustrated as header processing function 63 and key release request 64 in Figure 3 and described at page 13, lines 5-8 and at lines 29-31. The header processing function “coordinates obtaining the ability to decrypt the message encryption key K from the key release agent”. The key release request 64 is described as containing the key ciphertext and the key related information in the description of the present application at page 11, lines 31-33 and page 13, lines 29-31.

The decryptor comprises “means for making decryptor information available to the key release agent”, examples of which are described at page 13, lines 5-9 and lines 29-30 and page 18 lines 15 to 23). The decryptor information is for use by the key release agent to locate decryptor authorization logic (page 14, lines 11 to 15) stored externally to the key release request. The logic is to be applied in determining whether or not to release the decryption key, an example of which is described on page 15, lines 21-25.

The decryptor comprises “means for receiving a key release response”, an example of which is described at page 13 lines 9-11 and page 13 line 33 to page 14 line 1, with specific reference to header processing function 63 and key release response 66 in Figure 3.

Claim 35 is dependent upon claim 33 and recites the additional limitation of “further comprising means for using the decryption key to decrypt the data ciphertext”, an example of which is described at page 13, lines 11-15, with specific reference to decryption function 68 “which can decrypt ciphertext 44 in the event that the required symmetric key is made available in a key release response 66 from the key release agent”.

Claim 37 is dependent upon claim 33 and recites the further limitation of “further comprising means for decrypting at least a portion of the key release response containing an encrypted version of the decryption key using a private key of a second {public key,

private key} pair to recover the decryption key”, an example of which is described at page 13 line 33 to page 14 line 6, again with specific reference to decryption function 68.

Claim 38 is directed to a key release agent (KRA), an example of which is shown in Figure 1 identified with reference character 14 or the KRA of Figure 4. A corresponding description is located at page 14, lines 8-18 of the present application. An example of operation of the key release processor 80 illustrated in Figure 4 is located at page 16 line 22 to page 18 line 4, with reference to Figure 7.

The KRA comprises “means for receiving from a decryptor a key ciphertext and key related information in respect of a key used to encrypt the key ciphertext”, an example of which is the key release processor 80 in Figure 4 described at page 14, lines 9-10, with specific reference to key release request 64. Block 7-1 in Figure 7 and corresponding description at page 16, lines 24-27 also discloses reception of the key release request containing the encryption block header and identifier DI.

The KRA comprises “means for locating decryptor authorization logic stored externally to the decryptor with use of the key related information”, an example of which is described at page 16 line 27 to page 17 line 12, as would be performed by the key release processor 80.

The KRA comprises “means for obtaining decryptor information in respect of the decryptor”, an example of which is illustrated in block 7-6 of Figure 7 and described in further detail on page 17, lines 7-10, as would be performed by the key release processor 80.

The KRA comprises “means for deciding based on decryptor information and the decryptor authorization logic whether decryption of the ciphertext is to be permitted”, an example of which is illustrated in block 7-7 of Figure 7 at page 17 line 4 to page 18 line 4 and at page 15, lines 21 to 25, as would be performed by the key release processor 80.

Claim 41 is dependent upon claim 38 and further recites “decrypting means for decrypting the key ciphertext”, an example of which is illustrated in block 7-11 of

Figure 7 and described in further detail on page 17, lines 26-33, as would be performed by the key release processor 80.


The KRA further comprises “encryption means for re-encrypting the key using a public key of a {public key, private key} pair to produce a re-encrypted key, the private key of which is available to the decryptor”, an example of which is illustrated in block 7-12 of Figure 7 and described in further detail on page 17 line 34 to page 18 line 3, as would be performed by the key release processor 80.

The KRA further comprises “means for sending the re-encrypted key to the decryptor”, an example of which is illustrated in block 7-13 of Figure 7 and described in further detail on page 18, lines 3-4, as would be performed by the key release processor 80.

Claim 42 is dependent upon claim 38 and recites the additional limitation of “means for applying decryptor authorization logic associated with each public key used to encrypt the decryption key to the decryptor information for determining whether the decryptor should be permitted access to the decryption key”, an example of which is described at page 17, lines 7-26, with specific reference to block 7-7 in Figure 7, as would be performed by the key release processor 80.

Respectfully submitted,

GLENN LANGFORD

By 
Mark S. Starzomski
Reg. No. 62,411
Tel.: (613) 232-2486, Ext. 327

Smart & Biggar
P.O. Box 2999, Station D
900-55 Metcalfe Street
Ottawa, Ontario K1P 5Y6

Date: August 20, 2008

MSS:mcg